Assistant - Exhibit

A Balanced Key Management

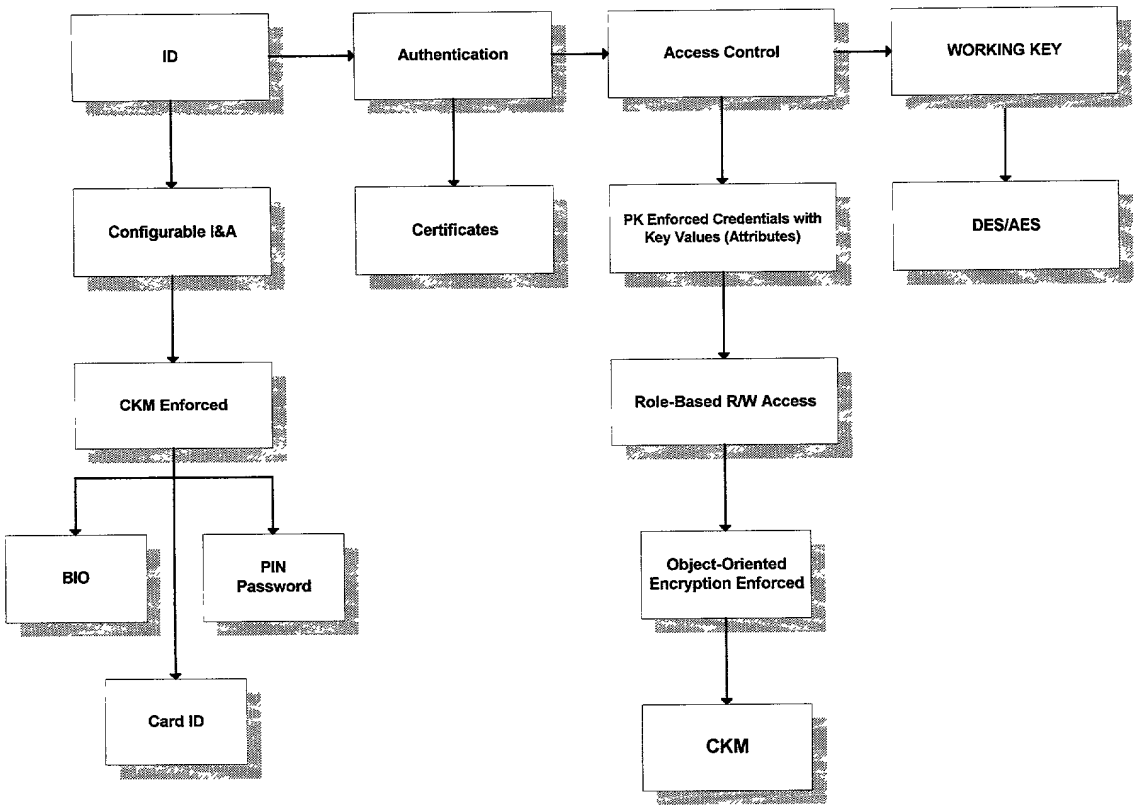


FIG. 1

Page 25 of 35 - 5/5/2004 12:52:35 PM

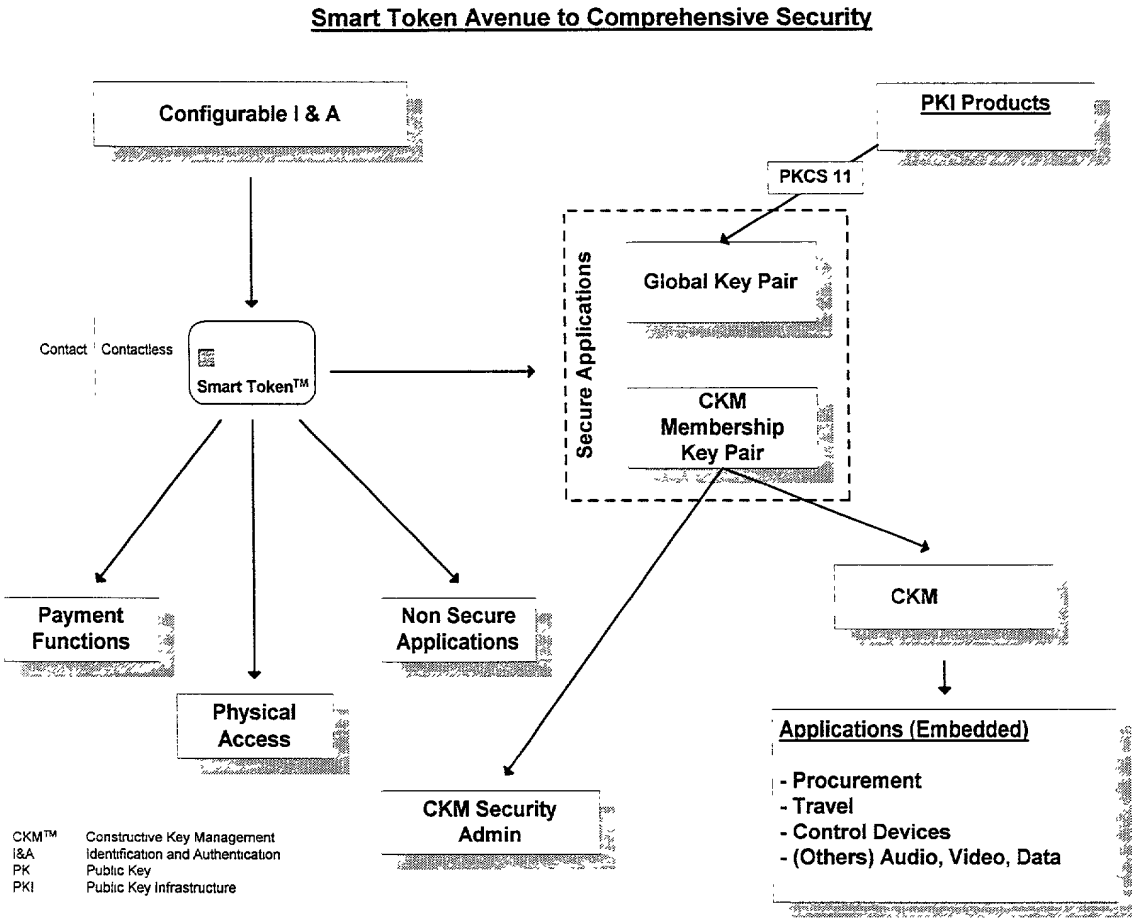
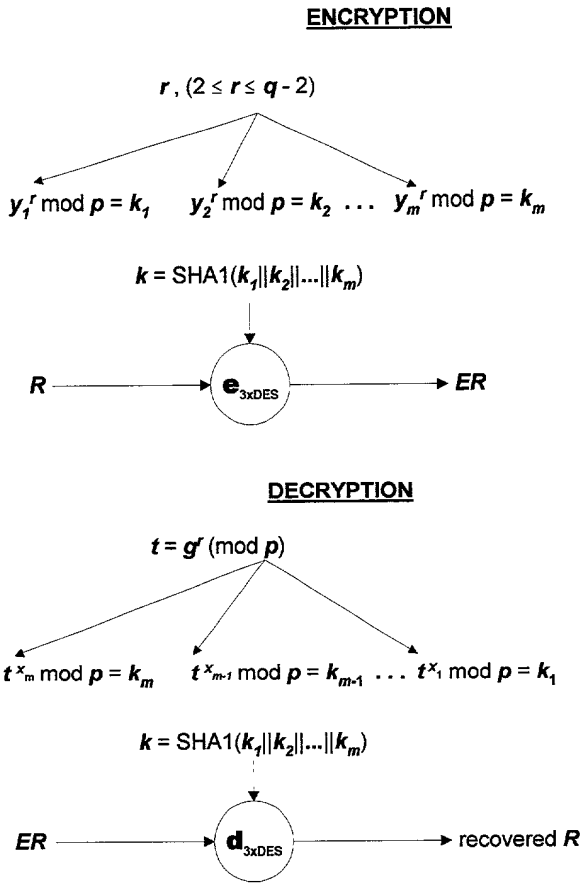


FIG. 2

Diffie-Hellman Random Value Encryption and Decryption



Legend:

p	Diffie-Hellman prime modulus
q	Diffie-Hellman 160-bit prime
g	generator of group Z_p
m	number of labels
k_i	i^{th} derived key
k	two-key 3xDES key
r	Ephemeral Private Key
R	Random Value
ER	Encrypted Random Value
t	Ephemeral Public Key

FIG. 3

Document ID: US 2004/0202324 A1

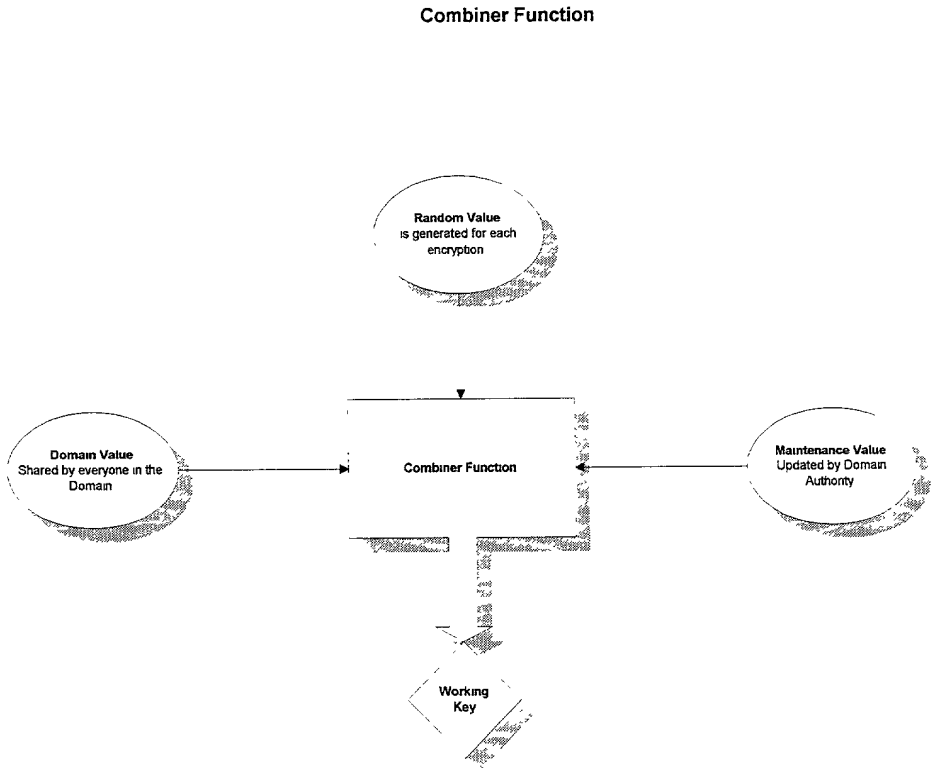
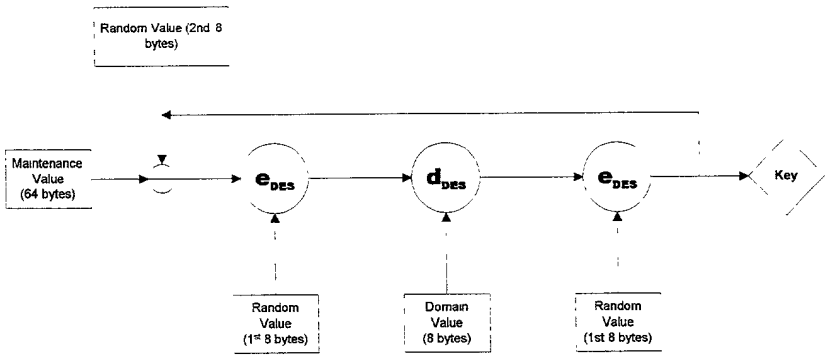


FIG. 4

Combiner Function Using Triple DES CBC Mode



Legend

e_{DES} DES encryption
d_{DES} DES decryption
$\oplus$ Exclusive-OR

FIG. 5

20050235125

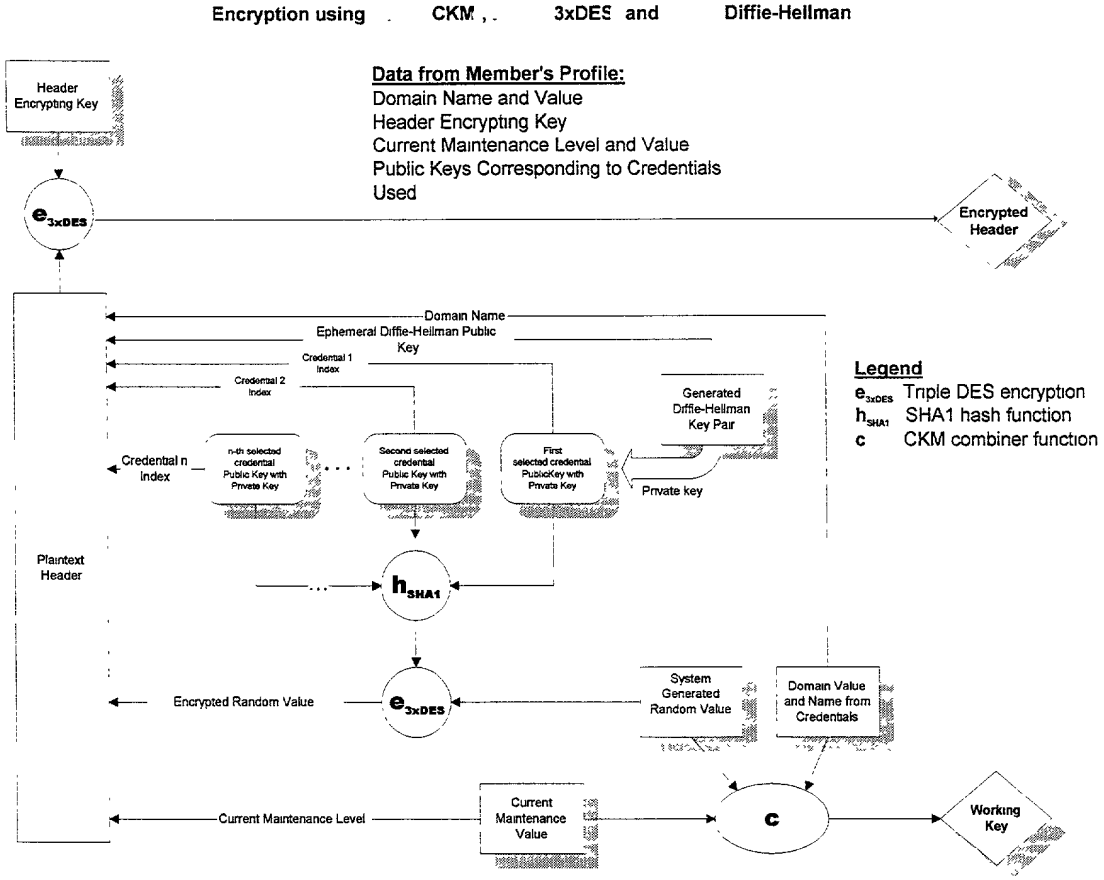
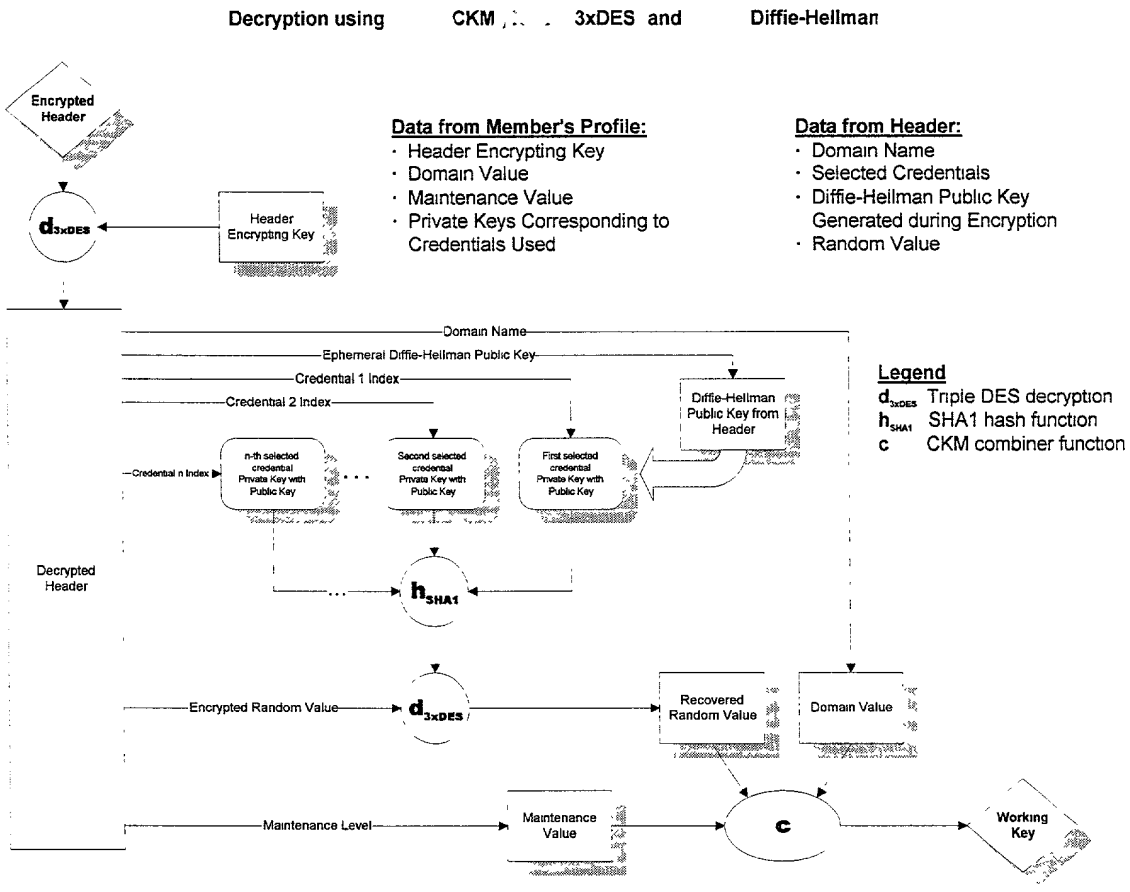


FIG. 6

FIG. 7


Decryption using CKM , 3xDES and Diffie-Hellman
Encrypted Header
d_{3xDES}
Header Encrypting Key
Data from Member's Profile:
· Header Encrypting Key
· Domain Value
· Maintenance Value
· Private Keys Corresponding to Credentials Used
Data from Header:
· Domain Name
· Selected Credentials
· Diffie-Hellman Public Key Generated during Encryption
· Random Value
Domain Name
Ephemeral Diffie-Hellman Public Key
Credential 1 Index
Credential 2 Index
Credential n Index
n-th selected credential Private Key with Public Key
Second selected credential Private Key with Public Key
First selected credential Private Key with Public Key
Diffie-Hellman Public Key from Header
Legend
d_{3xDES} Triple DES decryption
h_{SHA1} SHA1 hash function
c CKM combiner function
Decrypted Header
h_{SHA1}
Encrypted Random Value
d_{3xDES}
Recovered Random Value
Domain Value
Maintenance Level
Maintenance Value
c
Working Key

Encryption using CKM , 3xDES and RSA

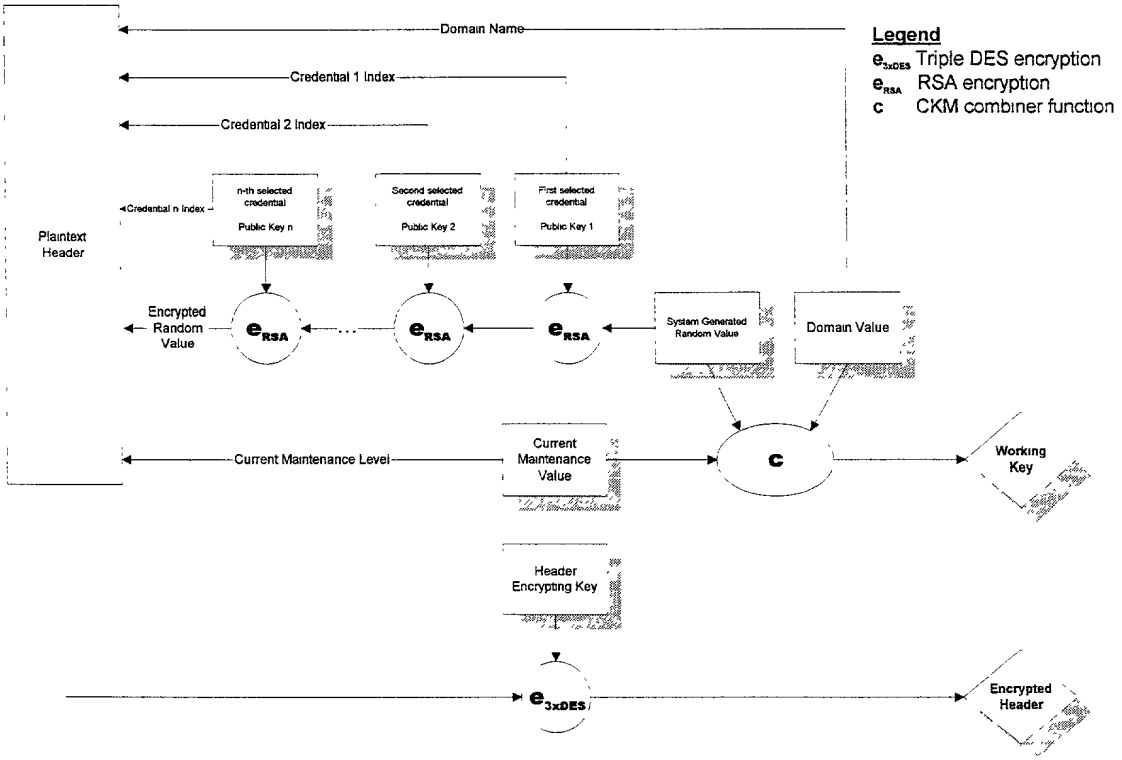


FIG. 8

Decryption using CKM , . 3xDES and RSA

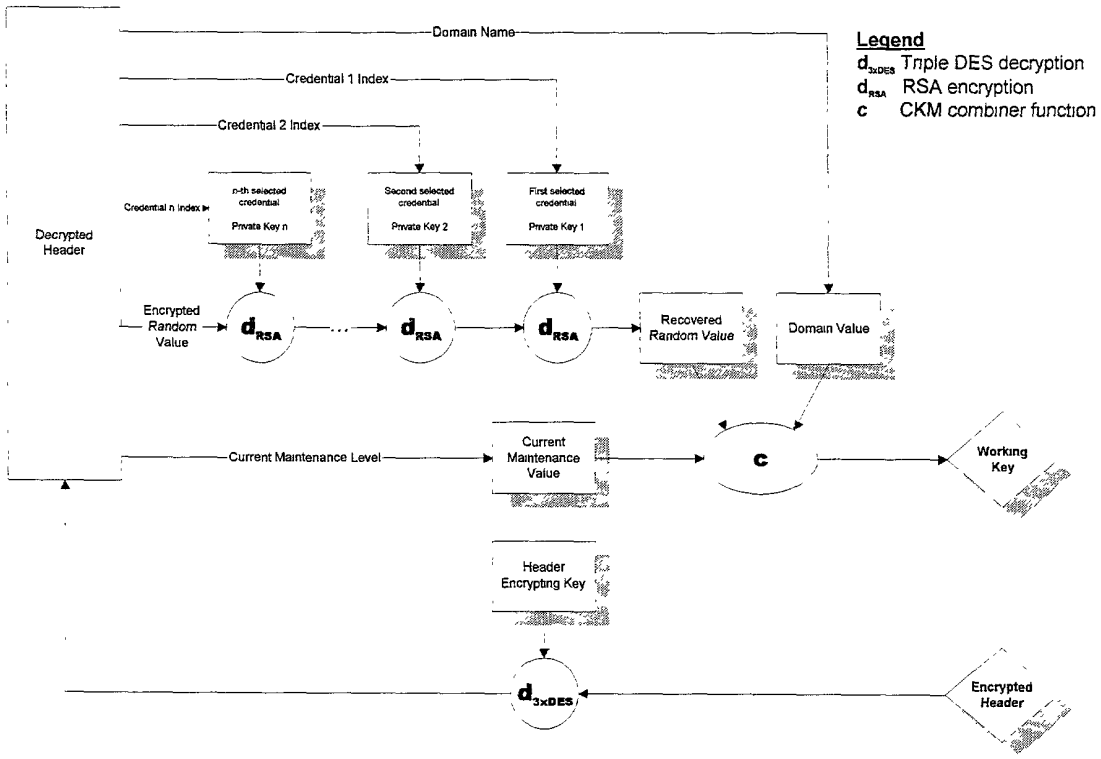


FIG. 9

FIG. 10

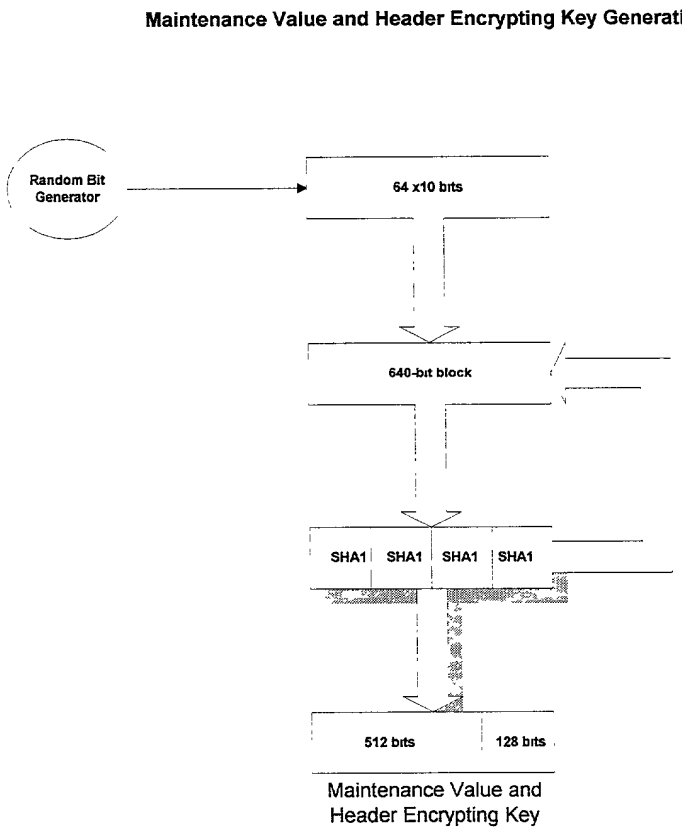

Maintenance Value and Header Encrypting Key Generation
Random Bit Generator
64 x10 bits
640-bit block
SHA1
SHA1
SHA1
SHA1
512 bits
128 bits
Maintenance Value and Header Encrypting Key

FIG. 11

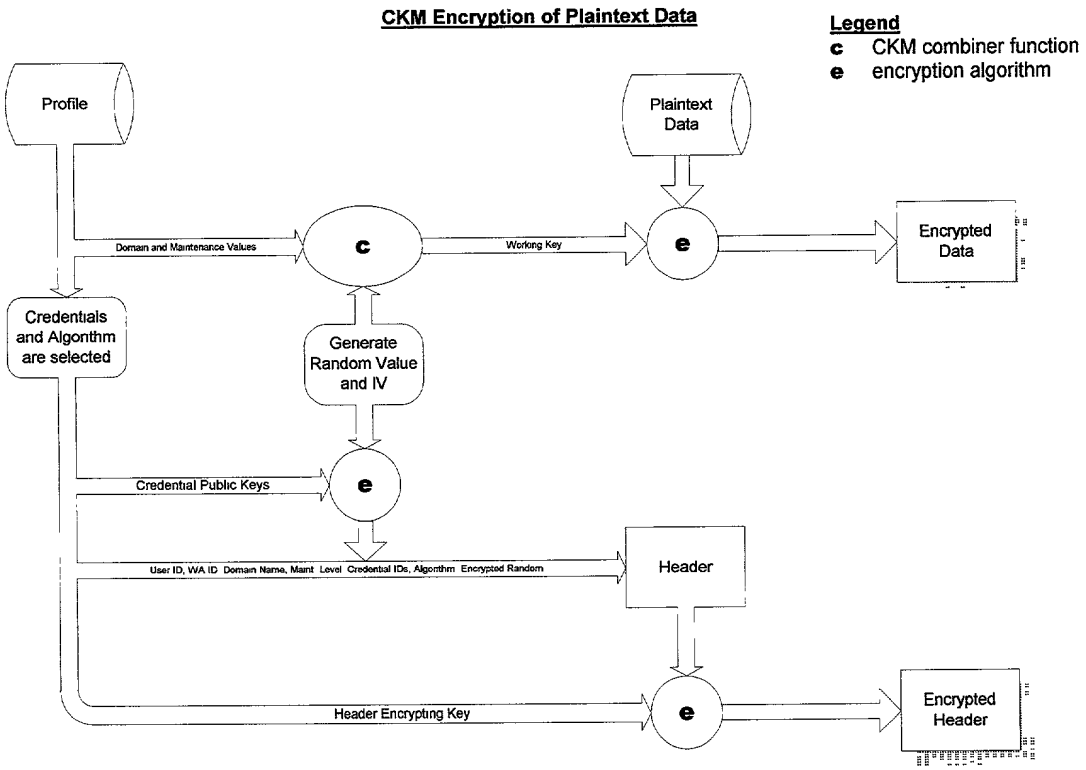

CKM Encryption of Plaintext Data
Legend
c CKM combiner function
e encryption algorithm
Profile
Plaintext Data
Domain and Maintenance Values
c
Working Key
e
Encrypted Data
Credentials and Algorithm are selected
Generate Random Value and IV
Credential Public Keys
e
User ID, WA ID Domain Name, Maint Level Credential IDs, Algorithm Encrypted Random
Header
Header Encrypting Key
e
Encrypted Header

FIG. 12

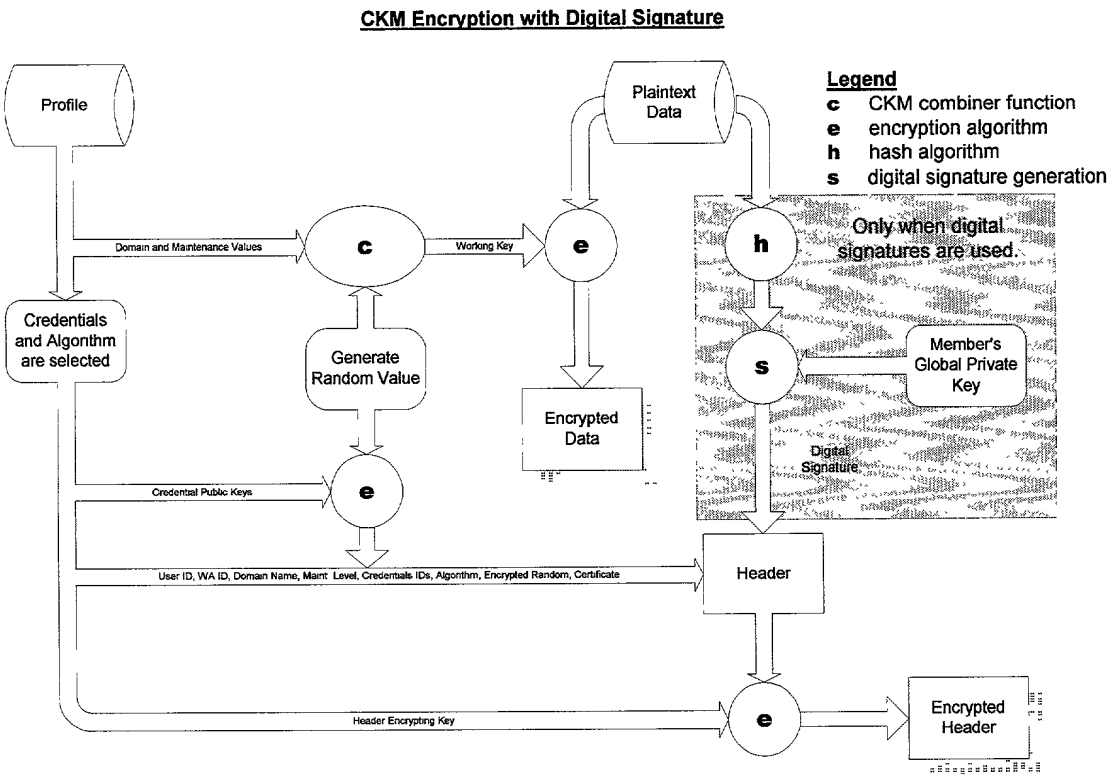
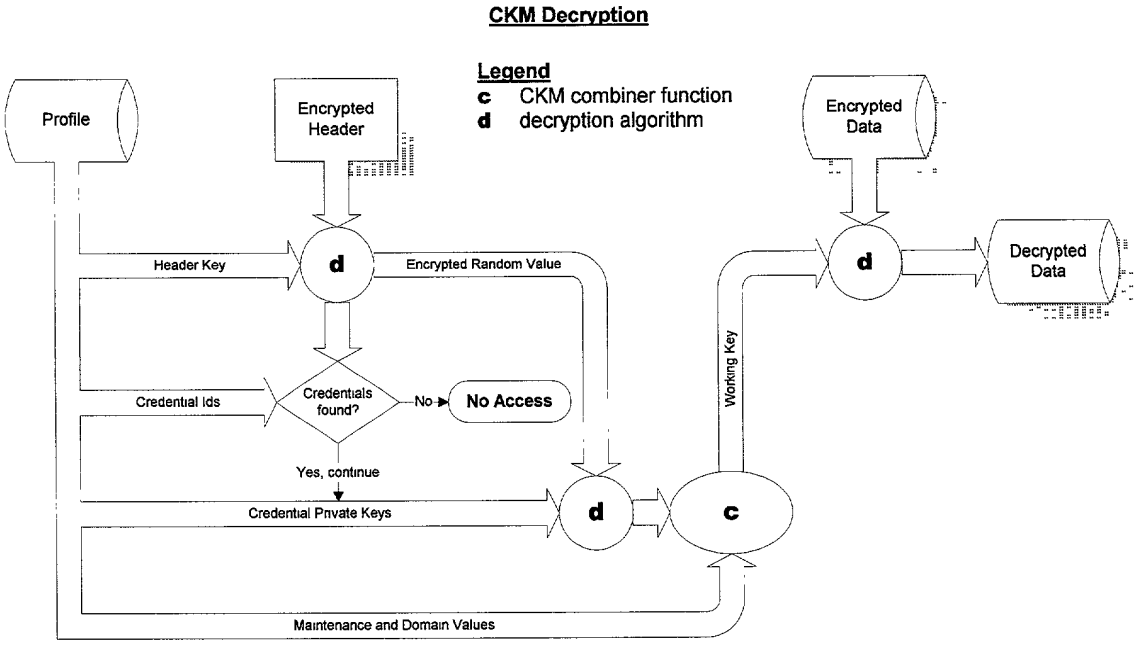

CKM Encryption with Digital Signature
Profile
Plaintext Data
Legend
c CKM combiner function
e encryption algorithm
h hash algorithm
s digital signature generation
Domain and Maintenance Values
c
Working Key
e
h
Only when digital signatures are used.
Credentials and Algonthm are selected
Generate Random Value
Encrypted Data
s
Member's Global Private Key
Digital Signature
Credential Public Keys
e
User ID, WA ID, Domain Name, Maint Level, Credentials IDs, Algorithm, Encrypted Random, Certificate
Header
Header Encrypting Key
e
Encrypted Header

FIG. 13


CKM Decryption
Legend
c CKM combiner function
d decryption algorithm
Profile
Encrypted Header
Encrypted Data
Header Key
d
Encrypted Random Value
d
Decrypted Data
Credential Ids
Credentials found?
No
No Access
Working Key
Yes, continue
Credential Private Keys
d
c
Maintenance and Domain Values

CKM Decryption with Digital Signature Verification

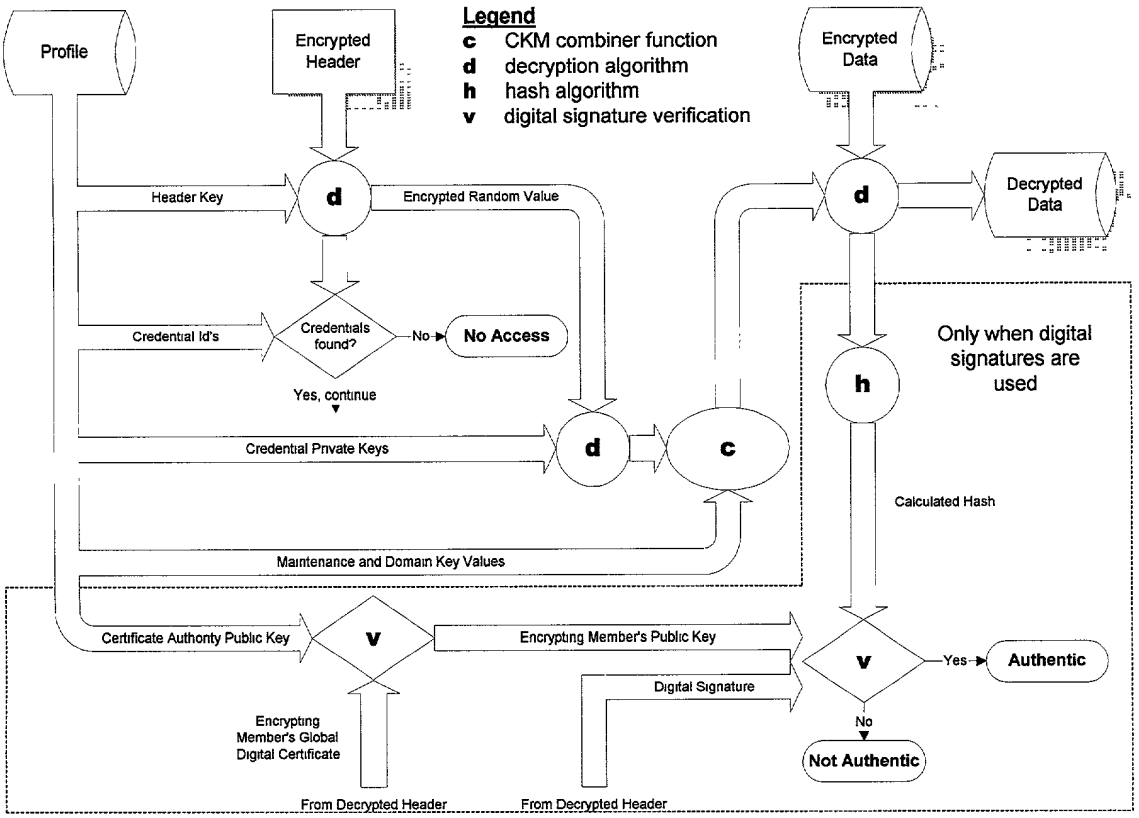


FIG. 14

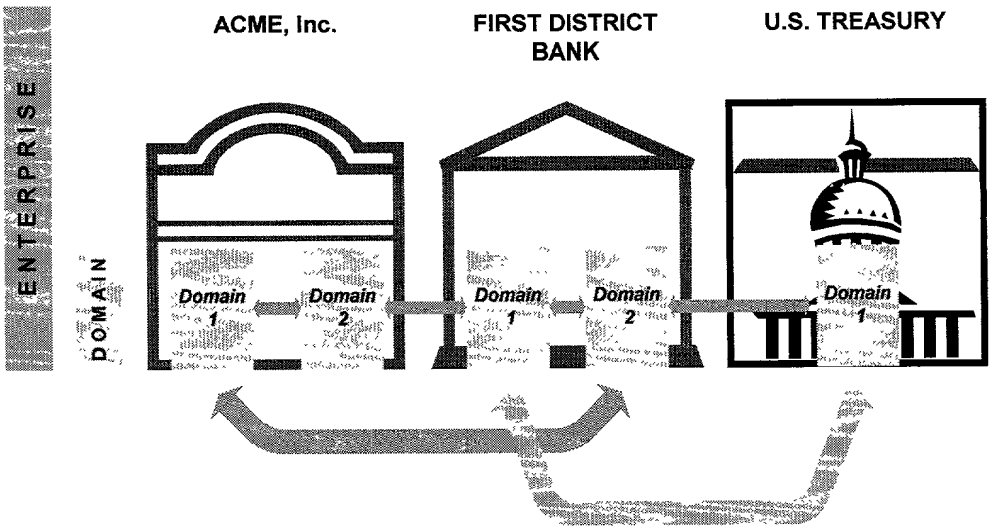


FIG. 15

US 6,253,328 B1

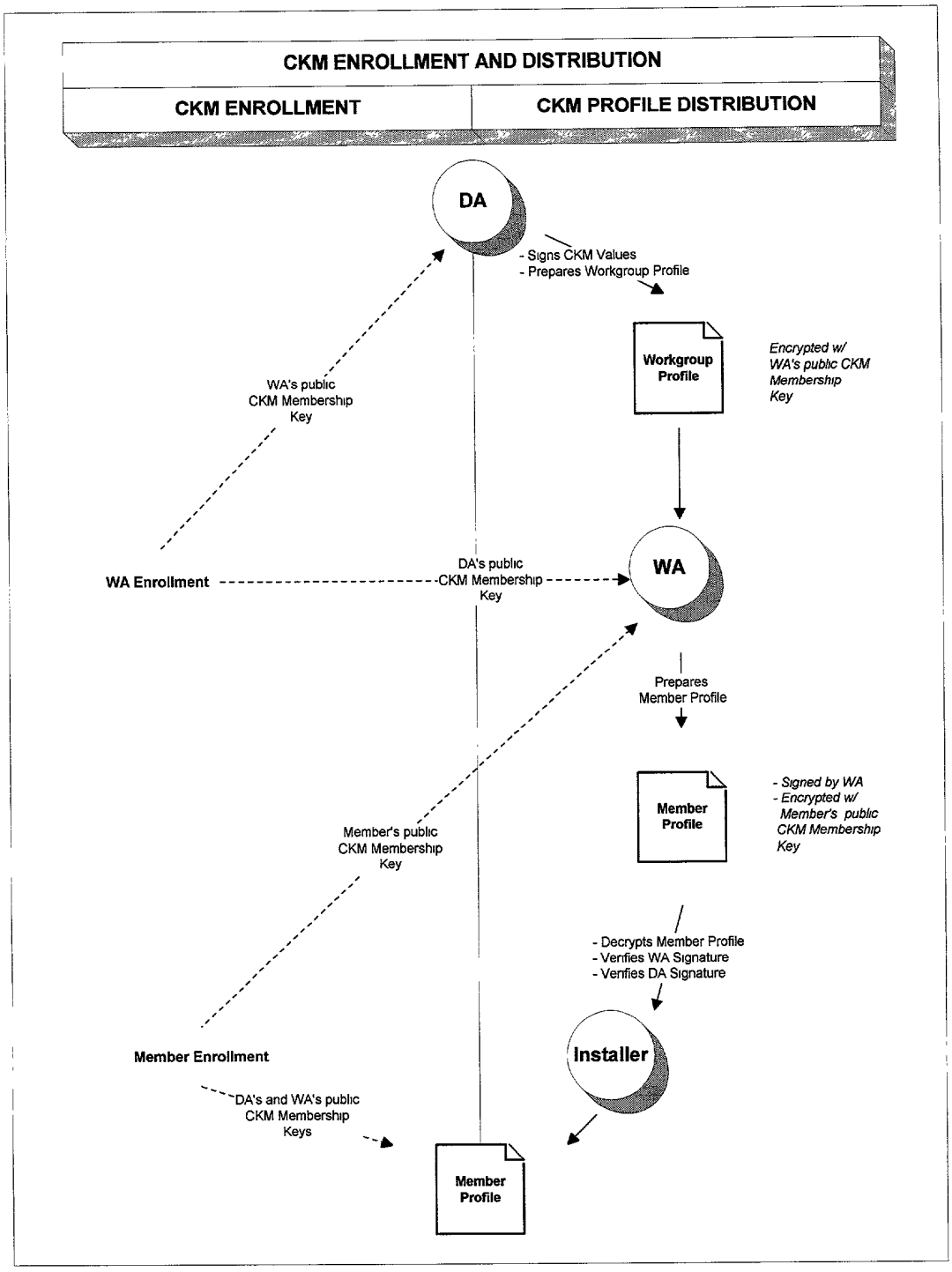

CKM ENROLLMENT AND DISTRIBUTION
CKM ENROLLMENT
CKM PROFILE DISTRIBUTION
DA
- Signs CKM Values
- Prepares Workgroup Profile
Workgroup Profile
Encrypted w/ WA's public CKM Membership Key
WA's public CKM Membership Key
WA Enrollment
DA's public CKM Membership Key
WA
Prepares Member Profile
Member Profile
- Signed by WA
- Encrypted w/ Member's public CKM Membership Key
Member's public CKM Membership Key
- Decrypts Member Profile
- Verifies WA Signature
- Verifies DA Signature
Installer
Member Enrollment
DA's and WA's public CKM Membership Keys
Member Profile

FIG. 16

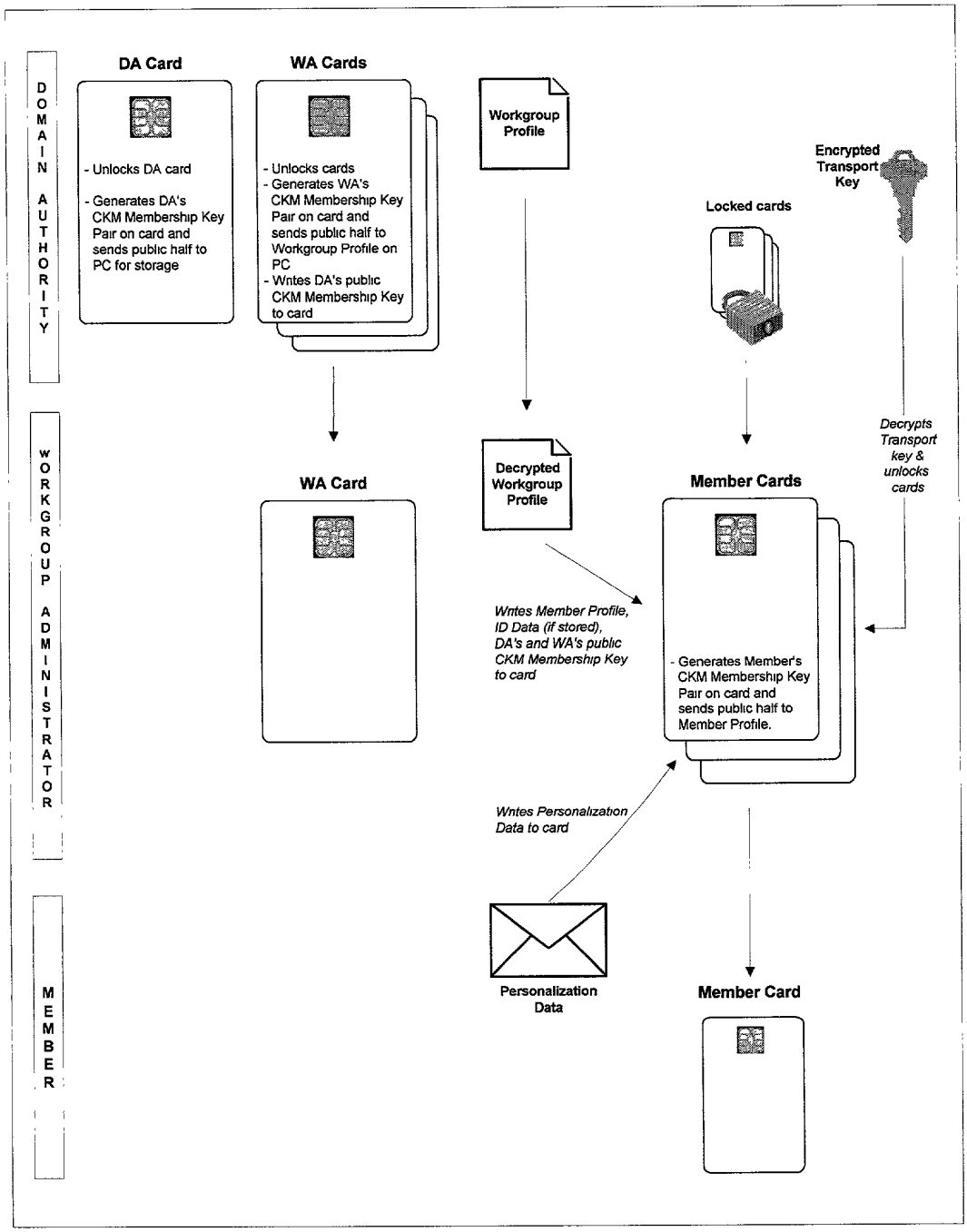

DOMAIN AUTHORITY
WORKGROUP ADMINISTRATOR
MEMBER
DA Card
- Unlocks DA card
- Generates DA's CKM Membership Key Pair on card and sends public half to PC for storage
WA Cards
- Unlocks cards
- Generates WA's CKM Membership Key Pair on card and sends public half to Workgroup Profile on PC
- Writes DA's public CKM Membership Key to card
Workgroup Profile
Encrypted Transport Key
Locked cards
Decrypts Transport key & unlocks cards
WA Card
Decrypted Workgroup Profile
Member Cards
Writes Member Profile, ID Data (if stored), DA's and WA's public CKM Membership Key to card
- Generates Member's CKM Membership Key Pair on card and sends public half to Member Profile.
Writes Personalization Data to card
Personalization Data
Member Card

FIG. 17

FIG. 18

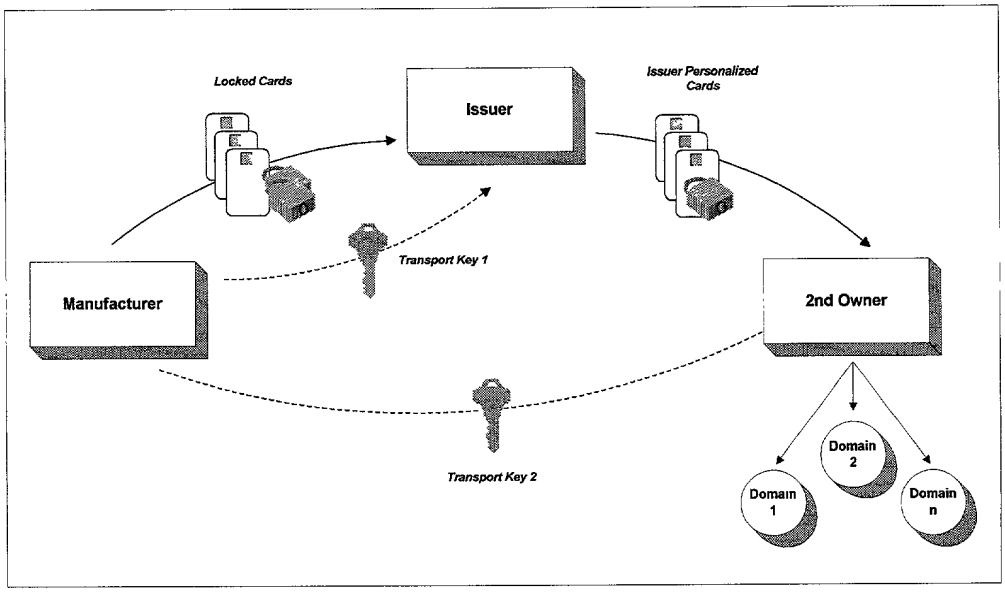

Locked Cards
Issuer
Issuer Personalized Cards
Transport Key 1
Manufacturer
2nd Owner
Transport Key 2
Domain 1
Domain 2
Domain n

FIG. 19

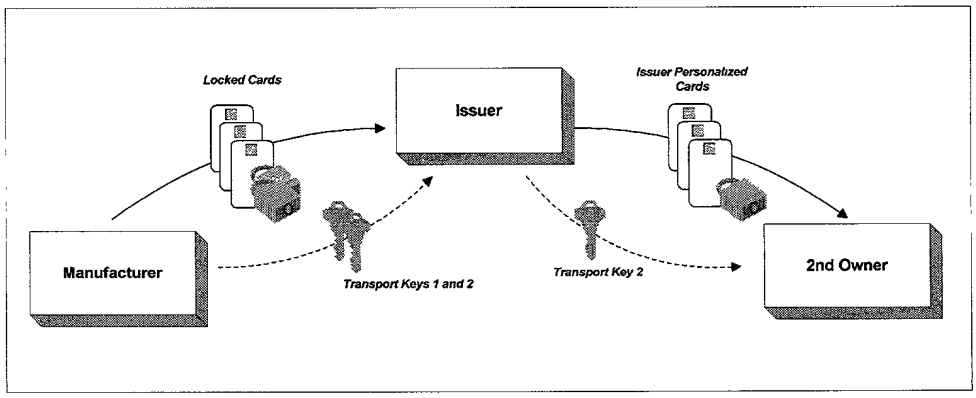

Locked Cards
Issuer
Issuer Personalized Cards
Manufacturer
Transport Keys 1 and 2
Transport Key 2
2nd Owner

FIG. 20

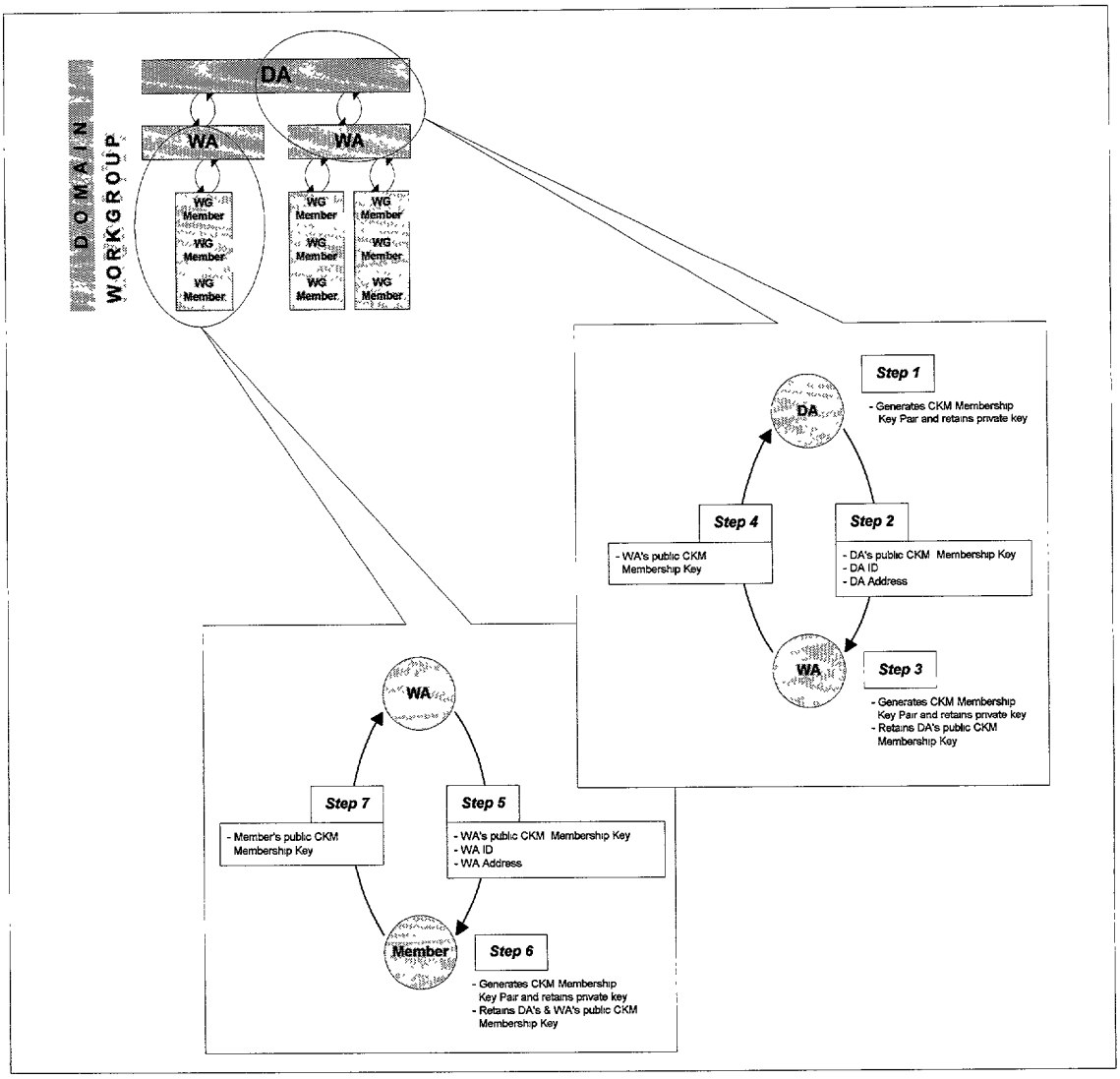

DOMAIN
WORKGROUP
DA
WA
WA
WG Member
WG Member
WG Member
WG Member
WG Member
WG Member
WG Member
WG Member
WG Member
Step 1
- Generates CKM Membership Key Pair and retains private key
DA
Step 4
- WA's public CKM Membership Key
Step 2
- DA's public CKM Membership Key
- DA ID
- DA Address
WA
Step 3
- Generates CKM Membership Key Pair and retains private key
- Retains DA's public CKM Membership Key
WA
Step 7
- Member's public CKM Membership Key
Step 5
- WA's public CKM Membership Key
- WA ID
- WA Address
Member
Step 6
- Generates CKM Membership Key Pair and retains private key
- Retains DA's & WA's public CKM Membership Key

FIG. 21

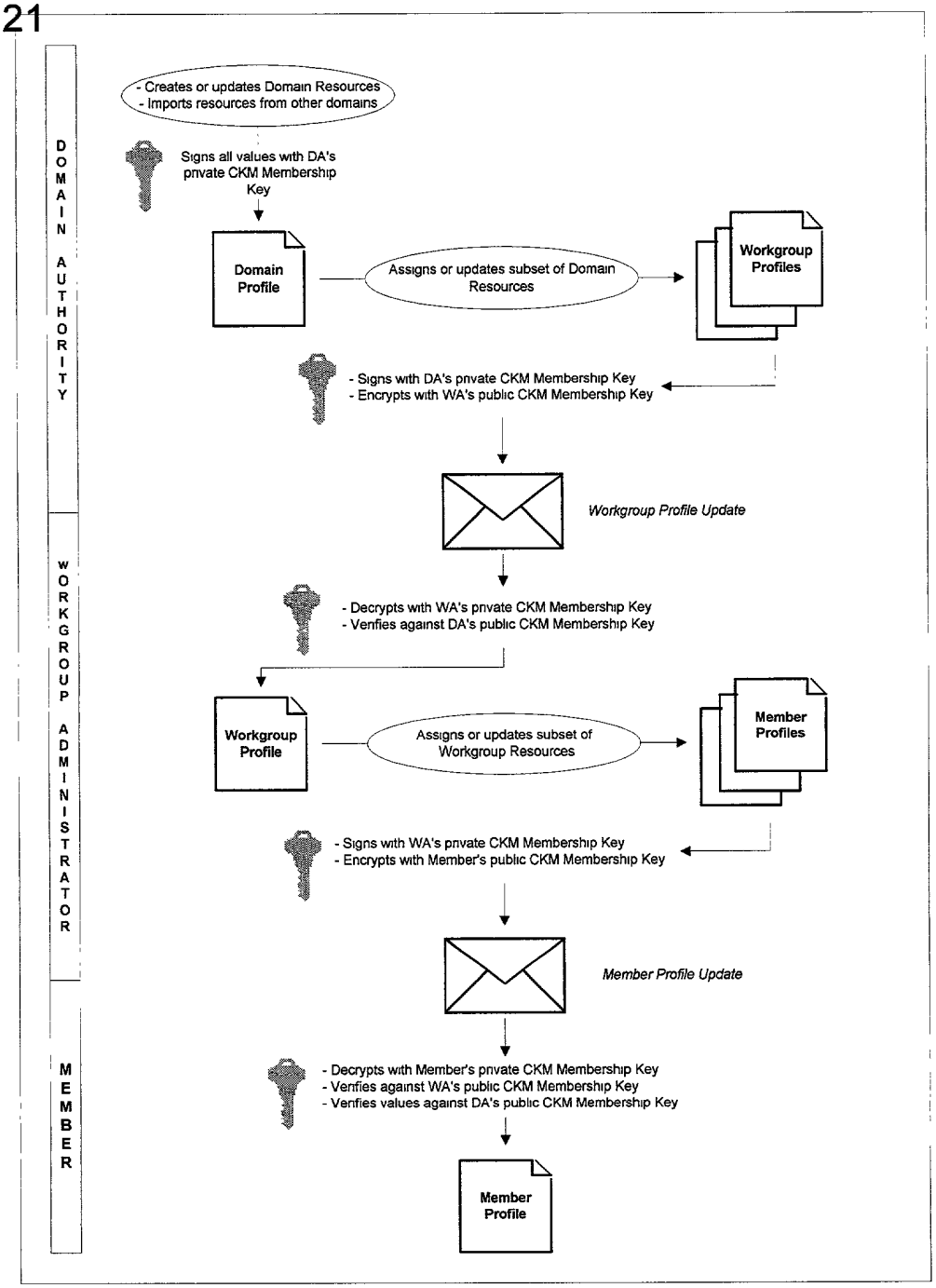

DOMAIN AUTHORITY
WORKGROUP ADMINISTRATOR
MEMBER
- Creates or updates Domain Resources
- Imports resources from other domains
Signs all values with DA's private CKM Membership Key
Domain Profile
Assigns or updates subset of Domain Resources
Workgroup Profiles
- Signs with DA's private CKM Membership Key
- Encrypts with WA's public CKM Membership Key
Workgroup Profile Update
- Decrypts with WA's private CKM Membership Key
- Verifies against DA's public CKM Membership Key
Workgroup Profile
Assigns or updates subset of Workgroup Resources
Member Profiles
- Signs with WA's private CKM Membership Key
- Encrypts with Member's public CKM Membership Key
Member Profile Update
- Decrypts with Member's private CKM Membership Key
- Verifies against WA's public CKM Membership Key
- Verifies values against DA's public CKM Membership Key
Member Profile

FIG. 22

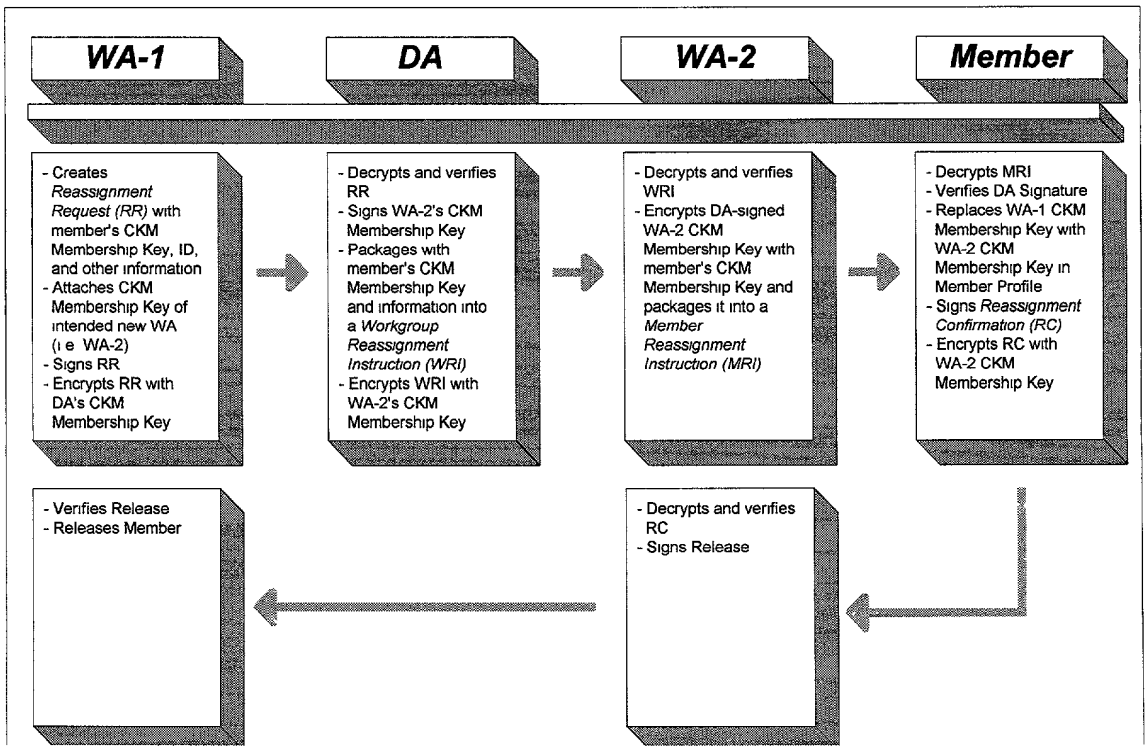
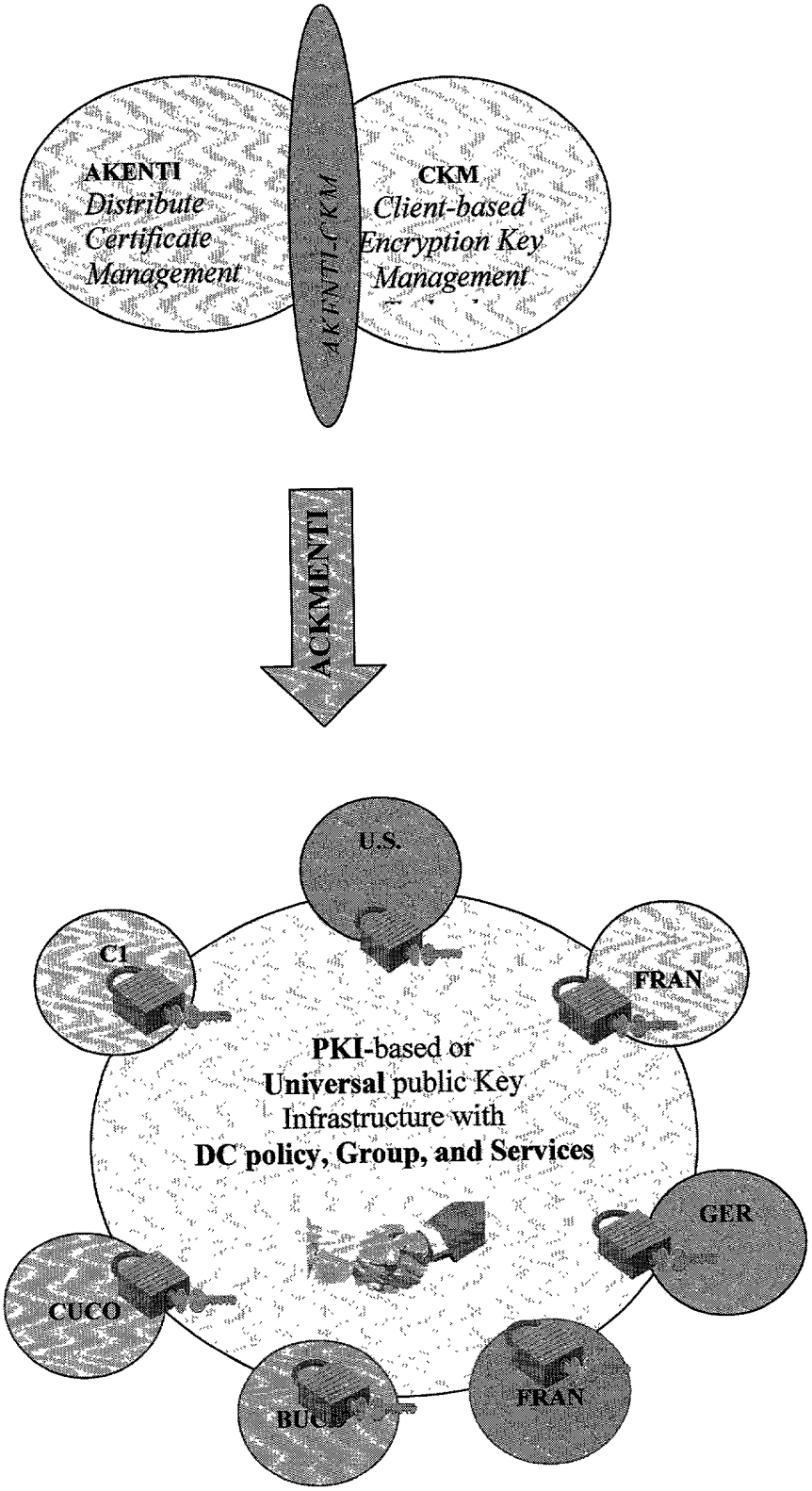

WA-1
DA
WA-2
Member
- Creates Reassignment Request (RR) with member's CKM Membership Key, ID, and other information
- Attaches CKM Membership Key of intended new WA (i e WA-2)
- Signs RR
- Encrypts RR with DA's CKM Membership Key
- Decrypts and verifies RR
- Signs WA-2's CKM Membership Key
- Packages with member's CKM Membership Key and information into a Workgroup Reassignment Instruction (WRI)
- Encrypts WRI with WA-2's CKM Membership Key
- Decrypts and verifies WRI
- Encrypts DA-signed WA-2 CKM Membership Key with member's CKM Membership Key and packages it into a Member Reassignment Instruction (MRI)
- Decrypts MRI
- Verifies DA Signature
- Replaces WA-1 CKM Membership Key with WA-2 CKM Membership Key in Member Profile
- Signs Reassignment Confirmation (RC)
- Encrypts RC with WA-2 CKM Membership Key
- Verifies Release
- Releases Member
- Decrypts and verifies RC
- Signs Release

FIG. 23



D-5526-05453

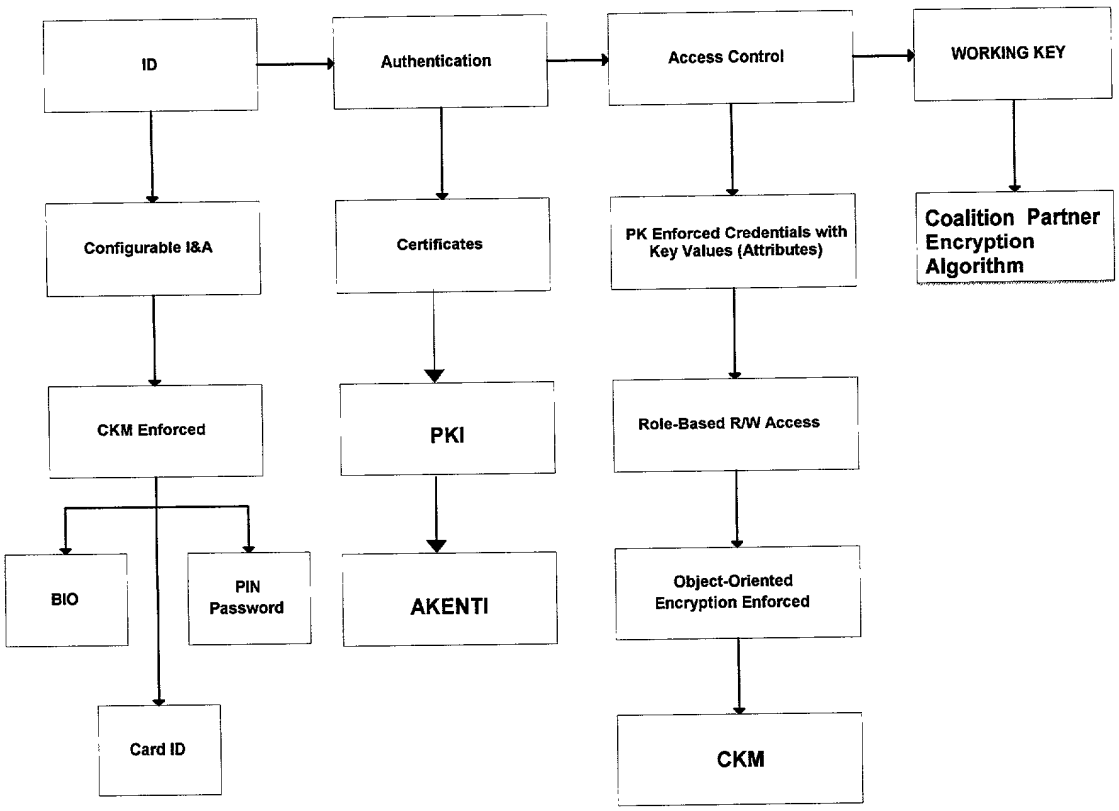

ID
Authentication
Access Control
WORKING KEY
Configurable I&A
Certificates
PK Enforced Credentials with Key Values (Attributes)
Coalition Partner Encryption Algorithm
CKM Enforced
PKI
Role-Based R/W Access
BIO
PIN Password
AKENTI
Object-Oriented Encryption Enforced
Card ID
CKM

FIG. 24

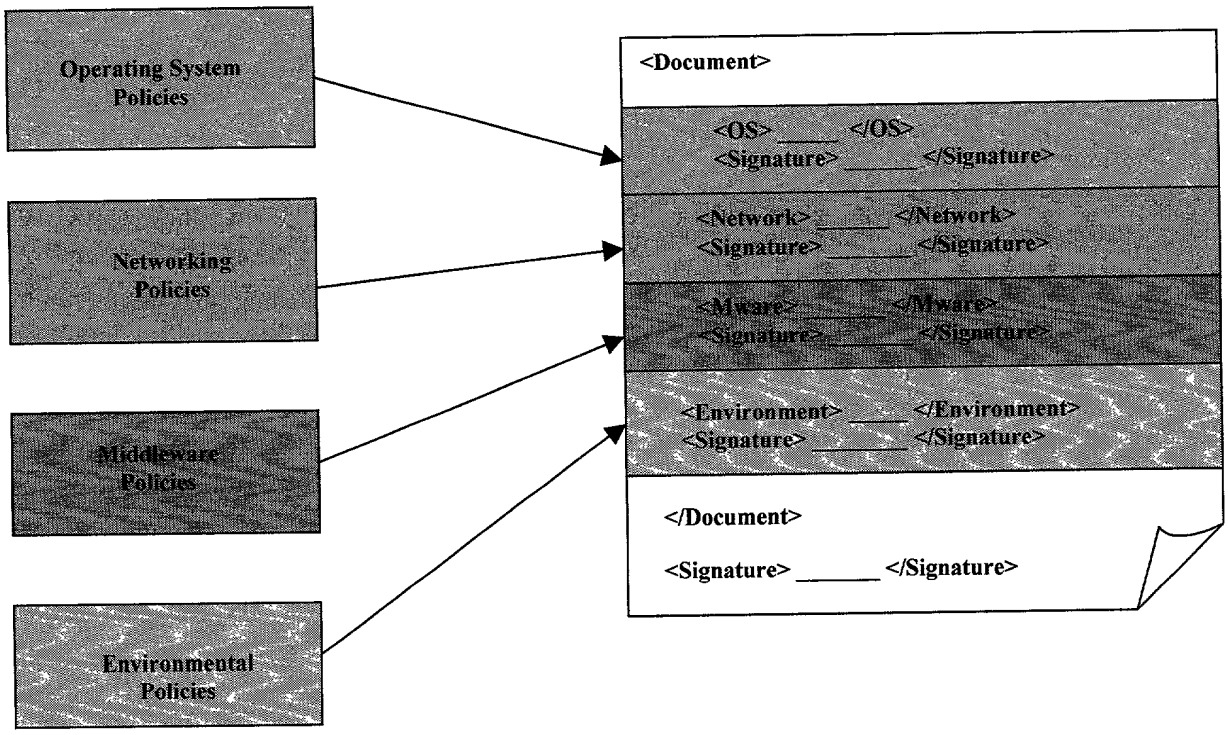

Operating System Policies
Networking Policies
Middleware Policies
Environmental Policies
<Document>
<OS> _____ </OS>
<Signature> _____ </Signature>
<Network> _____ </Network>
<Signature> _____ </Signature>
<Mware> _____ </Mware>
<Signature> _____ </Signature>
<Environment> _____ </Environment>
<Signature> _____ </Signature>
</Document>
<Signature> _____ </Signature>

FIG. 25

FIG. 26

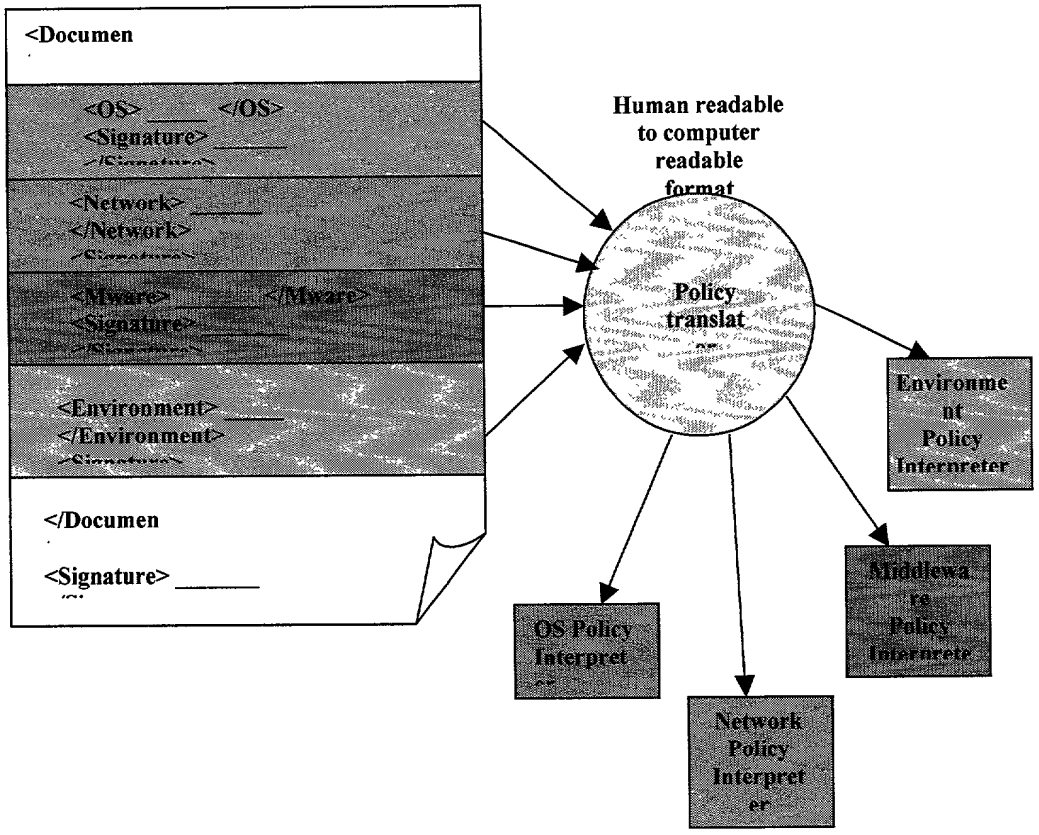
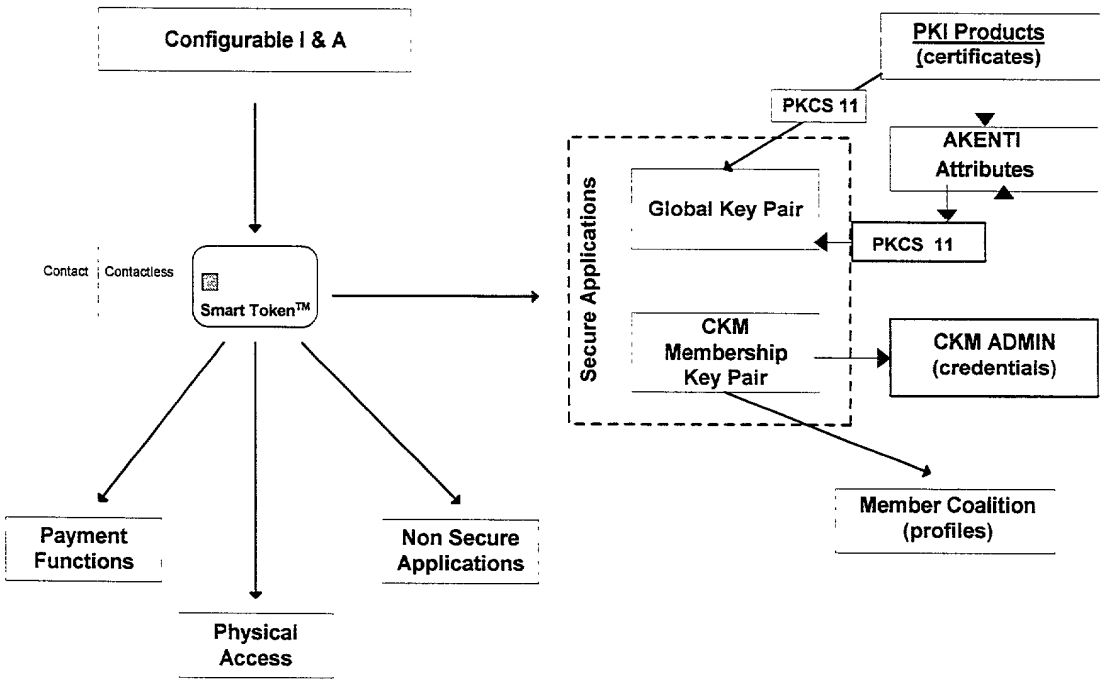

<Documen
<OS> _____ </OS>
<Signature> _____
<Network> _____
</Network>
<Mware> _____ </Mware>
<Signature> _____
<Environment> _____
</Environment>
</Documen
<Signature> _____
Human readable to computer readable format
Policy translat
Environme nt Policy Interpreter
Middlewa re Policy Interprete
OS Policy Interpret er
Network Policy Interpret er

FIG. 27



CKM™	Constructive Key Management
I&A	Identification and Authentication
PK	Public Key
PKI	Public Key Infrastructure

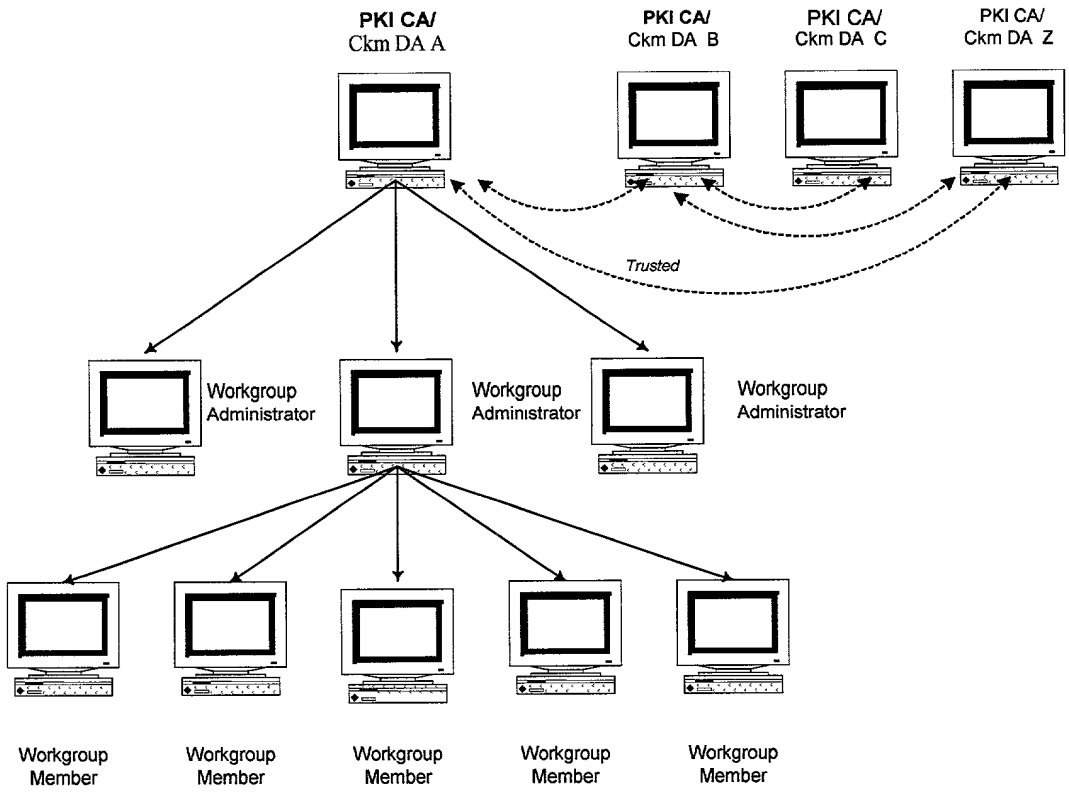

PKI CA/
Ckm DA A
PKI CA/
Ckm DA B
PKI CA/
Ckm DA C
PKI CA/
Ckm DA Z
Trusted
Workgroup
Administrator
Workgroup
Administrator
Workgroup
Administrator
Workgroup
Member
Workgroup
Member
Workgroup
Member
Workgroup
Member
Workgroup
Member

FIG. 28